OCTOBER 2023

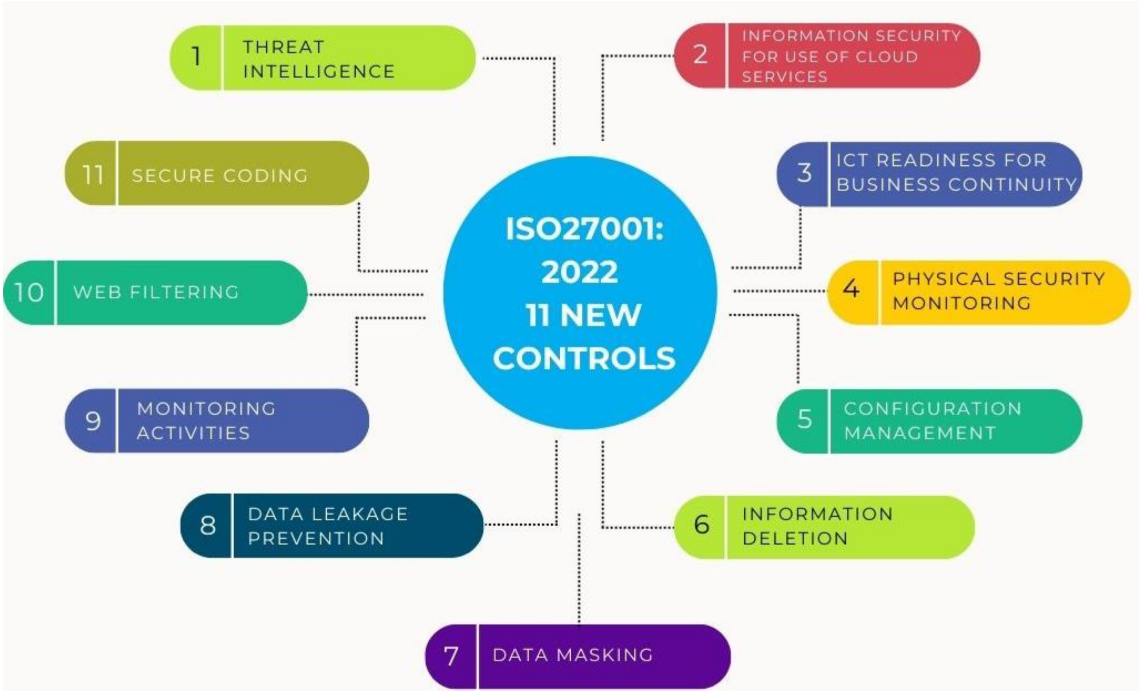
MOORE NEWSLETTER

Staying On Top For Potential Information Security Risk - The Key Updates And Implications Of The Revised ISO27001

In the past few years, the threat landscape had developed into a broader spectrum, reaching from classic attack patterns such as ransomware attack and data breaches to more advanced techniques like AI-driven attacks and IoT threats, thereby affecting organisations globally by possessing unforeseen consequences both financially and non-financially. These consequences include financial loss, reputation damage, and business operations disruption. Thus, a reliable and well known information security management system (ISMS) like ISO27001 should be implemented to protect firms from cyber threats.

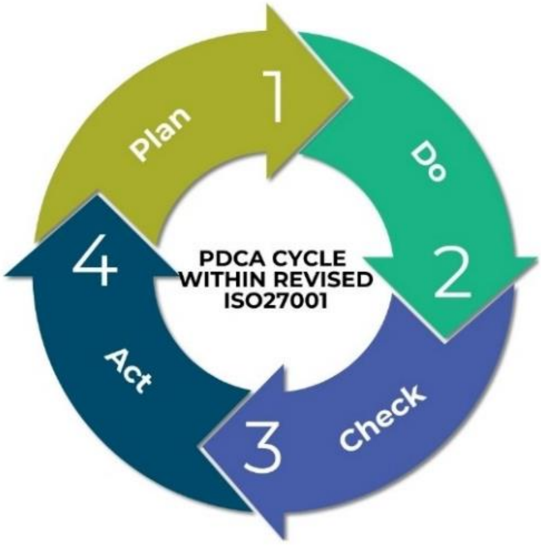
ISO27001 is a systematic approach consisting of people, processes, and technology, focusing on protecting three essential aspects of information, including confidentiality, integrity, and availability. Increasingly, global firms including Fortune 500 companies placed a high emphasis on information security with a 450% growth rate in the adoption of ISO 27001. The global standard specifies an effective ISMS to help all companies, regardless of their size, type, or nature, safeguarding their data systems and information assets.

Certifying your ISMS to the revised ISO27001 standard not only demonstrates your commitment to data security but also grants you a competitive advantage through accredited certification bodies like the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC). In 2022, ISO and IEC revised ISO27001 and consolidated the original 14 control domains into four themes: **organisational controls**, **people controls**, **physical controls**, and **technological controls**. Furthermore, the revision enables organisations to better address emerging risks and align their security practices with the evolving cybersecurity landscape through the introduction of 11 new controls as shown below:


ISO27001: 2022 11 NEW CONTROLS
1 THREAT INTELLIGENCE
2 INFORMATION SECURITY FOR USE OF CLOUD SERVICES
3 ICT READINESS FOR BUSINESS CONTINUITY
4 PHYSICAL SECURITY MONITORING
5 CONFIGURATION MANAGEMENT
6 INFORMATION DELETION
7 DATA MASKING
8 DATA LEAKAGE PREVENTION
9 MONITORING ACTIVITIES
10 WEB FILTERING
11 SECURE CODING

Methodology behind the implementation of ISO27001

Before implementing the ISMS standard, firms should understand the **PDCA (Plan-Do-Check-Act) cycle** as a foundation for the continuous improvement of an ISMS and ensure firms can continuously improve their ISMS through feedback and experiential insights. More importantly, the PDCA cycle is at the core of all ISO standards and applied throughout the clauses of ISO27001 to plan, implement, evaluate, and make improvements, thereby ensuring the effectiveness and continual improvement of the ISMS with four key phases explained briefly below:



Plan phase: Firms comprehend the context, leadership and commitment towards the ISO27001 implementation, develop plans to address risks and create resources to spread information security awareness. These elements extend support to one another to establish ISO27001 in the internal environment, promoting a collective effort towards its implementation.

Do phase: Organisations translate planned activities into practical action. This involves carrying out the implementation of controls, processes, and procedures that were established during the design phase. The primary objective is to execute the strategies and measures outlined in the ISMS to effectively mitigate information security risks and vulnerabilities.

Check phase: Involves continuous monitoring and evaluation of ISMS effectiveness. This include activities like identifying security breaches, measuring performance, and conducting internal audits to discover areas for improvement. The performance evaluation usually will be conducted in the form of audit to ensure that a firm's ISMS comply with the ISO27001 standard.

Act phase: Companies undertake preventive and corrective actions in response to the findings of internal audits, monitoring, and other evaluations.

Benefits of obtaining ISO27001:2022 certification

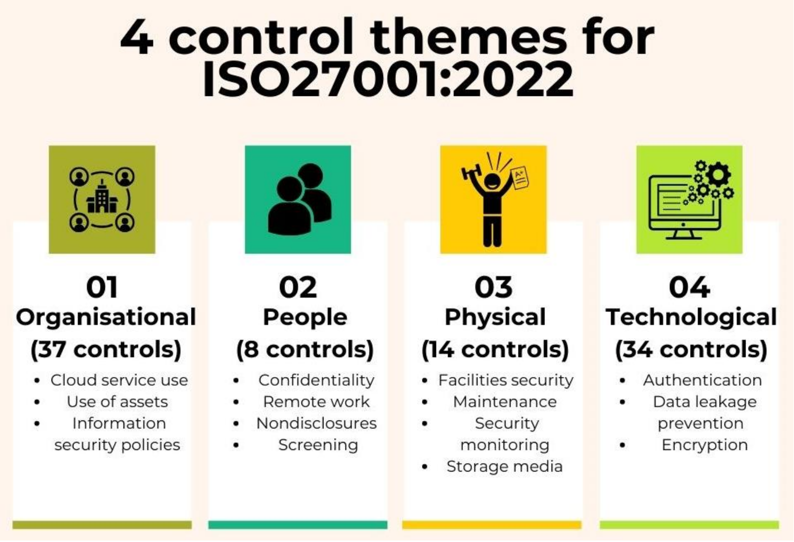
1. Prevention of security breaches and cost savings through targeted controls and mitigation of cyber risks.
2. Centralisation of compliance efforts, streamlining activities, and meeting regulatory obligations like General Data Protection Regulation (GDPR) and National Institute of Standards and Technology (NIST).
3. Enhancement of credibility is achieved by demonstrating a commitment to robust information security practices, which in turn builds trust among customers and stakeholders.
4. Provision of a comprehensive framework for securing data across various formats and protecting against unauthorised access and data breaches.
5. Facilitation of compliance and seamless integration of security processes through identifiable control attributes in new controls.
6. Structured approach to information security management, ensuring systematic security management, alignment with business objectives, and continuous improvement through regular evaluations and corrective actions.

It is important to keep in mind that organisations currently holding ISO 27001:2013 certification have until 31 October 2025, to transit to the new 2022 revision. This allows them three years to understand the changes, implement them within their information security management systems (ISMS), and undergo the certification process based on the updated standard. However, new certification applicants may continue to be audited against the 2013 revision only until 31 October 2023.

Revisions in ISO27001:2022

The recent revisions from clause four to ten of the revised ISO27001 standard have been implemented to improve global firm's practices in managing information security and ensure the utmost safeguarding of valuable data. This section will explore the four new themes and the significant updates that will further combat evolving threats.

Instead of having 14 categories of controls, both revised ISO27001 and ISO27002 are now grouped into four categories - organisational, people, physical and technological. Simultaneously, the number of controls have reduced from 114 to 93. A brief explanation of the four themes will be illustrated on the next page:



4 control themes for ISO27001:2022

01 Organisational (37 controls)

- Cloud service use
- Use of assets
- Information security policies

02 People (8 controls)

- Confidentiality
- Remote work
- Nondisclosures
- Screening

03 Physical (14 controls)

- Facilities security
- Maintenance
- Security monitoring
- Storage media

04 Technological (34 controls)

- Authentication
- Data leakage prevention
- Encryption

Organisational: Cover information security policies, asset management, cloud service use, identity management, management and evidence collection.

People: Assist in controlling how workers deal with confidential information in the course of their daily work.

Physical: Protect against physical and environmental threats like natural disasters, theft and intentional destruction.

Technological: Focuses on properly securing technology through various approaches, including access rights, network security, and data masking.

Understanding the 11 controls

11 new Annex A controls		
New controls	**Control theme**	**Description**
1. Threat intelligence (A 5.7)	Organisational control	Establish procedures to collect and analyse threat data for proactive risk management and incident response.
2. Information security for use of cloud services (A 5.23)	Organisational control	Align information security requirements for the acquisition, use, and management of cloud services.
3. ICT readiness for business continuity (A 5.30)	Organisational control	Plan, implement, and test ICT systems to ensure information integrity during disruptions.
4. Physical security monitoring (A 7.4)	Physical control	Continuously monitor premises to prevent unauthorised physical access and protect assets.
5. Configuration management (A 8.9)	Technological control	Establish, monitor, and review configurations to maintain the desired state of IT infrastructure and systems.
6. Information deletion (A 8.10)	Technological control	Properly delete obsolete information to maintain data hygiene and mitigate risks associated with unnecessary data retention.
7. Data masking (A 8.11)	Technological control	Utilise substitute data for testing or non-production purposes to protect sensitive information while maintaining usability.
8. Data leakage prevention (A 8.12)	Technological control	Implement measures to prevent unauthorised disclosure of sensitive information and protect data assets.
9. Monitoring activities (A 8.16)	Technological control	Establish a comprehensive monitoring system to proactively detect and respond to security incidents.
10. Web filtering (A 8.23)	Technological control	Manage access to external websites to minimise exposure to malicious content and enhance information security.
11. Secure coding (A 8.28)	Technological control	Apply secure coding principles to minimise vulnerabilities and ensure software application security.

Summary of the changes in each clause of ISO 27001:2022

Clause 4 (Context of the organisation)

Clause 4.2 (Understanding the needs and expectations of interested parties) now requires greater clarification of the requirements of interested parties by adding item (c), which specifies that the information security management system should address these requirements explicitly.

Clause 4.4 (Information security management system) introduces additional wording that emphasises the inclusion of processes necessary for maintaining and improving the ISMS, aligning it with other ISO standards like ISO 9001:2015 and ISO 22301:2019. This update enhances the focus on processes.

Clause 5 (Leadership)

Clause 5.3 (Organisational roles, responsibilities and authorities) clarifies the responsibilities and authorities for roles relevant to information security. Top management is now required to ensure that these roles are assigned and communicated within the organisation. ISO 27001 implicitly or explicitly mandates three specific roles: ISMS manager, performance reporter to top management, and internal auditor.

Clause 6 (Planning)

Clause 6.2 (Information security objectives and planning to achieve them) introduces item (d), which mandates the monitoring of objectives throughout the lifecycle of the certification. Additionally, item (g) emphasises that objectives should be available as documented information, making Clause 6.2 a mandatory document.

Clause 6.3 (Planning od changes) specifies that changes to the information security management system should be carried out in a planned manner when the organisation determines the need for such changes.

Clause 7 (Support)

Clause 7.4 (Communication) removes items (d) and (e), which previously addressed the processes and personnel responsible for communication. Item (d) is amended to focus on how communication should be carried out.

Clause 8 (Operation)

Clause 8.1 (Operational planning and control) revises the language to align with Clause 6.2 (Information security objectives and planning to achieve them), removing the necessity to implement plans for accomplishing objectives. The updated requirement ensures that externally provided processes, products, or services relevant to the ISMS are controlled.

Clause 9 (Performance evaluation)

Clause 9.1 (Monitoring, measurement, analysis and evaluation) provides clarification on what qualifies as a "valid" result by stating that the methods selected should produce comparable and reproducible results. The evaluation of information security performance and the effectiveness of the ISMS is also emphasised.

Clause 9.3 (Management review) introduces item 9.3 (c), which clarifies that inputs from interested parties for management review should be about their needs, expectations, and relevance to the ISMS.

Clause 10 (Improvement)

Clause 10 (Improvement) now reverses the order, with 10.1 focusing on continual improvement and 10.2 on nonconformity and corrective action. These changes in the ISO 27001:2022 standard aim to provide greater clarity, alignment, and emphasis on processes, enabling organisations to enhance their information security management practices effectively.

Moore IT & Cybersecurity Services

Why work with us?

We are a global advisory network, with offices and member firms across the globe. Backed by our international network, we provide clients with comprehensive cybersecurity solutions and expertise from security vulnerability assessment to system penetration testing to protect them from modern cyber threats.

Our team is composed of professionals with practical and solid knowledge and experience. They are certified holders or members of professional bodies such as CISA, CISM, CRISC, CISSP, CIPP(A), CEH, OSCP and GPEN.

Our clients range from SME to listed companies from wide variety of industry, and public sector including government bureau and authorities. Through our extensive sector knowledge, we provide comprehensive advice to suit each client's goals.

Our IT & Cybersecurity Service Team

PATRICK ROZARIO
Managing Director

T +852 2738 7769
E patrickrozario@moore.hk

KEVIN LAU
Principal

T +852 2738 4631
E kevinlau@moore.hk

Follow us on social media @moorehongkong

MOORE

www.moore.hk

We believe the information contained herein to be correct at the time of going to press, but we cannot accept any responsibility for any loss occasioned to any person as a result of action or refraining from action as a result of any item herein.